

REMARKS/ARGUMENTS

Favorable consideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 8-11 and 13-14 are pending in this application, with Claims 8, 9, 13 and 14 amended and Claim 12 cancelled by the present amendment.

In the outstanding Office Action, the Specification was objected to; Claims 8-14 were rejected under 35 U.S.C. § 101; Claims 8-9, 13-14 were rejected under 35 U.S.C. § 102 (b) as being anticipated by to Shamir (EP 0325238 A2); Claim 12 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Shamir, in view of Schneier (Applied Cryptography- Protocols, Algorithms and Source Code in C, 2nd Edition, pages 249-250) and Claims 10 and 11 were indicated as being allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim 8 is amended to recite the features of cancelled Claim 12. Claims 8, 9 and 13 are also amended to overcome the rejection under 35 U.S.C. § 101. No new matter is added.

Briefly recapitulating, amended Claim 8 is directed to an authentication process in which, *inter alia*, modulo n calculations are performed according to the “Chinese remainders” method.

Shamir describes a residue modulo n calculation. However, as noted in the Official Action, Shamir is silent about the use of the Chinese remainder. Schneier discloses a variety of cryptography protocols and discloses the use of the Chinese Remainder theorem. However, Schneier fails to disclose or suggest using the Chinese Remainder theorem in an authentication process. Applicants submit that a person having an ordinary skill in the art would not find in Schneier any indication or suggestion to perform the residue modulo n calculation in Shamir's invention by means of calculation according to the Chinese remainder method.

The Chinese remainder method is used in Applicants' invention to modulo calculate the prime factors of n . Shamir uses only residues modulo n even when n is a product of primes. Consequently, the algorithm of calculation of the claimed invention is different from Shamir's algorithm.

In the Chinese remainder method, to calculate $y = x^e \pmod{n}$, the algorithm according to the applicant invention starts by reducing x modulo each prime factor by calculating $x_p = x \pmod{p}$ and $x_q = x \pmod{q}$. The e is reduced modulo $(p-1)$ and $(q-1)$ by calculating $e_p = e \pmod{(p-1)}$ and $e_q = e \pmod{(q-1)}$, e being always lower than $(p-1)$ and $(q-1)$ and $e_p = e_q = e$. Then we calculate $y_p = x_p^{e_p} \pmod{p}$ and $y_q = x_q^{e_q} \pmod{q}$.

Moreover, the claimed invention is different from Shamir's method in respect of the effects and the advantages obtained by reducing x , e and n . In fact, when p and q are of similar size, each of the calculations (y_p and y_q) is about 8 times faster than the calculation of $y = x^e \pmod{n}$ when n and e are of similar size, 4 times faster when the size of e is lower or equal to the size of p .

On the whole, the use of the Chinese remainder leads to an acceleration of calculation by factor ranging from 3 to 4 or 1,5 to 2 depending on the size of e with regard to n and to p . Furthermore, when the number of primes factors (assumes to be' of similar sizes) is larger than 2 and equal to k , the acceleration factor is nearing k^2 in the first case (e and n of similar size) and close to k in the seconds case (e is lower than or equal to p)

MPEP §706.02(j) notes that to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when

combined) must teach or suggest all the claim limitations. Also, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Regarding cancelled Claim 12 (and now amended Claim 8), Applicants submit that the Official Action does not present a *prima facie* case of obviousness because both there is no motive to combine Shamir and Schneier achieve the features of Applicants' claimed invention.

In effect, the outstanding rejection of cancelled Claim 12 (and now included in amended Claim 8) does little more than attempt to show that parts of the inventive combination of Claim 12 were individually known in other arts and to suggest that such a showing is all that is necessary to establish a valid case of *prima facie* obviousness. The Federal Circuit recently reviewed such a rationale and dismissed it in *In re Rouffet*, 149 F. 3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998) as follows:

As this court has stated, "virtually all [inventions] are combinations of old elements." *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 698, 218 USPQ 865, 870 (Fed. Cir. 1983); see also *Richdel, Inc. v. Sunspool Corp.*, 714 F.2d 1573, 1579-80, 219 USPQ 8, 12 (Fed. Cir. 1983) ("Most, if not all, inventions are combinations and mostly of old elements."). Therefore an examiner may often find every element of a claimed invention in the prior art. If identification of each claimed element in the prior art were sufficient to negate patentability, very few patents would ever issue. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." *Sensonics, Inc. v. Aerosonic Corp.*, 81 F.3d 1566, 1570, 38 USPQ2d 1551, 1554 (Fed. Cir. 1996). To prevent the use of hindsight based on the invention to defeat patentability of the invention, this court requires the examiner to show a motivation to combine the references that create the case of obviousness. In other words, the examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. [emphasis added.]

There has been no such showing of those required reasons made in the rejection.

Accordingly, in view of the present amendment and in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action to that effect.


Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

GJM/MEMO/rca/jyh
I:\ATTY\MM\AMENDMENT\2623\211526US AMD.DOC



Gregory J. Maier
Attorney of Record
Registration No. 25,599

Michael E. Monaco
Registration No. 52,041